

The draft General Data Protection Regulation

from a DPA perspective

by Harald Zwingelberg

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Overview

- The draft general data protection regulation
- Up- and downsides of the current draft
- Selected concerns from a DPA view
- Conclusion

European General Data Protection Regulation

- One regulation for all EU Member States
- Binding and applicable without national implementation
- Draft issued January 25, 2012
- 91 Articles
- Current status: discussion phase

http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf



EUROPEAN COMMISSION

Brussels, 25.1.2012
COM(2012) 11 final

2012/0011 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

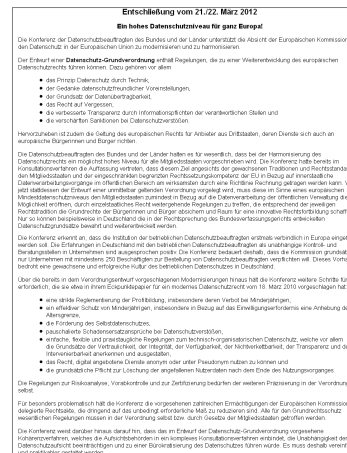
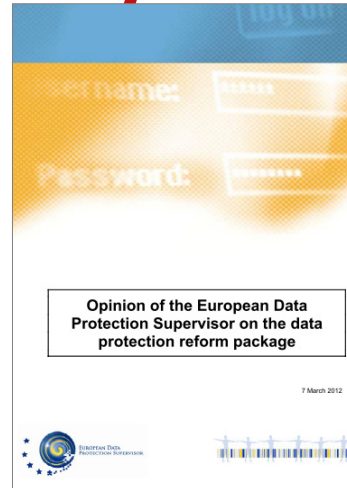
(Text with EEA relevance)

{SEC(2012) 72 final}

{SEC(2012) 73 final}

Selected responses from DPAs

- Responses from data protection authorities to the draft regulation
- EDPS: Opinion¹⁾
- Art. 29 Working Party: Working Paper 191²⁾
- German DPAs on national and federal level³⁾
- ...



1) http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf
 2) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf
 3) http://www.lida.brandenburg.de/sixcms/detail.php?gsid=bb1.c.284018.de&template=lda_entschl

Some highlights

- Art. 3: Territorial scope
- Art. 17: Right to be forgotten and to erasure
- Art. 18: Right to data portability
- Art. 31: Data breach notification

- Art. 10: Processing not allowing identification
- Art. 22: Responsibility of the controller
- Art. 23: Data protection by design and by default
- Art. 35 et seq.: Data protection officer

Advantages for data controllers

- Further harmonized rule set for legal certainty in cross-border transactions
- One stop shop: one harmonized law to adhere to and one DPA taking the lead in communication
- Documentation replaces notification
- Fewer bureaucracy for SMEs

Selected concerns from a DPA view

- Central questions left to be clarified by the Commission with delegated acts
- Minors / Representation of adults
- Threshold of 250 employees for SMEs
- Details for private data controllers missing (e.g. direct marketing)

Delegated acts: Aspects to be regulated

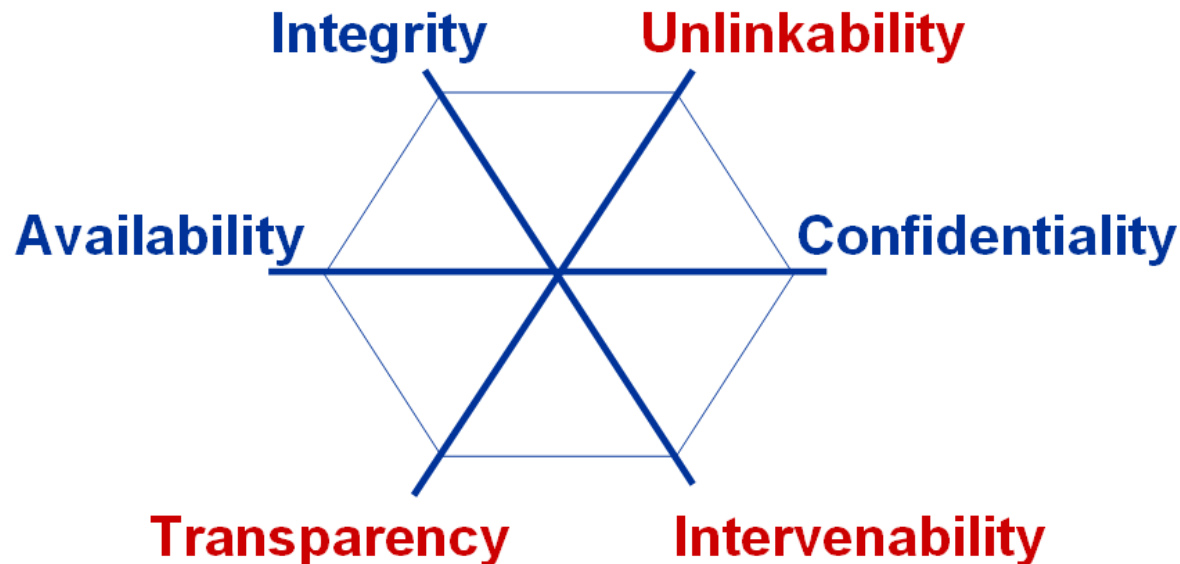
- Several questions are not governed by the regulation but to be clarified in delegated acts
- Central aspects that should be clarified in the regulation have been left open, too
- Time component as a problem
 - Legal uncertainty until delegated act is in force
 - But key points must be clarified by entry into force of the regulation
 - Commission should provide a roadmap for delegated acts in to be published in short, medium or long term


Delegated acts: privacy by design and default

- Privacy by Design and privacy by default are interesting concepts.
- Hard to enforce without further substantiation of the principle. Art 23 (2) does not add much beyond a restatement of the data minimisation principle
- Development of delegated act should involve EDPB and international standardisation bodies.

Delegated acts: Privacy by Design and Default

- Consider privacy protection goals for further specification:



- Suggestion by position paper of German DPA for regulation
- Accepted in principal for ISO standardisation
- More: today at 16:00, Room 2 tutorial by 



Delegated acts: technical and organisational measures, PETs

- Regulation offers opportunities to foster **privacy enhancing technologies** (PETs) in Art. 23 and Art. 30
- Clarifications need
 - Definition of “state of the art”
 - Statement on appropriate “costs of implementation”
 - What can be enforced / required by DPAs?
- Again: assessment with privacy protection goals useful to identify conflicts and/or synergy effects

Children / Representation

- Art. 8 clarifies the ability of children to consent into processing of personal data in online environments
- Age boundary of 13 years reasonably considers understanding of risks for own identity
- A European harmonisation was necessary
- Also educational measures for pupils are required but out of scope as EU does not have competence for this
- But representation has more aspects to consider ...

Children/ Representation

- Seeing the ageing population Art. 8 should be extended to delegation in general (self chosen delegates, advocates, ...)
- Open questions on delegation need to be answered in a medium term timeframe
 - Does parental veto overrule the minor's consent?
 - Does a legal guardian's vote also overrule an adult?
 - Delegator must act clearly in on behalf of the delegate. How document who did what without infringing privacy?
 - May a delegator control the delegate? How?



PrimeLife

For Questions on Delegation and Privacy see:
 M. Hansen, M. Raguse, K. Storf, H. Zwingelberg, Delegation for Privacy
 Management from Womb to Tomb – A European Perspective,
<http://www.springerlink.com/content/7w1471w58t275878/>

Threshold for SMEs

- Some requirements only apply to controllers with more than 250 employees
 - Art. 28 documentation
 - Art. 35 DPO
 - Art. 25 representative in Europe
 - and further references with regard to SMEs
- Current German solution
 - DPO to be installed with 10 employees involved with processing of personal data or always for scoring / profiling, or processing involves special categories of data not solely for a contractual duty

Threshold for SMEs

- Proposal: Replace exemption
 - Avoid discrimination of larger companies with less invasive data processing over SMEs with risky processing (e.g. internet start ups on behavioural advertising)
 - Take number of employees involved with processing and the type of data processed into account
- Content of documentation is needed as privacy policy as basis for informed consent anyway in many cases

Lawfulness of processing for direct marketing

- Lawfulness of processing, Art. 6 (a)-(f)
- Art. 6 (f) allows necessary processing for “legitimate interests pursued by a controller, except where such interest are overridden by the interest ... of the data subject ...”
- Is advertisement and direct marketing a legitimate interest? Is this interest overridden by fundamental rights?
- Preferably allow use of personal data for marketing only with prior consent (permission marketing)

Conclusion

- The draft Regulation brings data protection forward and unifies the protection level
- Adjustments for the online businesses have been made
- Clarifications necessary, commission is aware of those and is empowered to adopt delegated acts
- Corrosion of planned privacy features must be prevented
 - during the consultation phase for the regulation
 - during preparation of delegated acts

Thank you for your attention



Questions, comments, suggestions?

Contact:

Harald Zwingelberg

hzwingelberg@datenschutzzentrum.de

www.datenschutzzentrum.de

+49 (0)431 / 988-1228

ABC4Trust research results are to be
published at: www.abc4trust.eu